

FILED

MAY 17 2013

CLIFFORD J. PROUD
U.S. MAGISTRATE JUDGE
SOUTHERN DISTRICT OF ILLINOIS
EAST ST. LOUIS OFFICE

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF ILLINOIS

IN THE MATTER OF THE SEARCH OF)
)
One LG Model US670 cellular phone)
S/N: 103KPRW0111358, Seized)
From David G. Driskill at)
300 N. Jefferson St. Apartment 3,)
Jerseyville, Illinois 62052)

CRIMINAL NO. *13-M-6022-CJP*

**APPLICATION AND AFFIDAVIT
FOR SEARCH WARRANT**

I, David J. Wargo, being duly sworn depose and say:

I am a Special Agent of the Illinois State Police, and have reason to believe that on the property known as:

LG Model US670 cellular telephone (S/N: 103KPRW0111358) with the markings
"Made in Korea"

and which property was seized in Jersey County, within the Southern District of Illinois, there is now concealed certain property, including

SEE ATTACHED LIST ENTITLED "ATTACHMENT A"

which constitutes evidence of the commission of a criminal offense or which is contraband, the fruits of crime, or things otherwise criminally possessed, or which is designed or intended for use or which is or has been used as the means of committing an offense in violation of Title 18 United States Code § 2422(b), specifically evidence related to enticement of a minor and other sections of the United States criminal statutes. The facts to support the issuance of a search warrant are as follows:

AFFIDAVIT

1. I am a Special Agent of the Illinois State Police, and have been so employed for approximately 13 years. I am also a Special Federal Officer deputized by the United States Marshals Service to conduct investigations involving the victimization of children. My current assignment is forensic examiner/investigator with the United States Secret Service – Southern Illinois Cyber-crime Unit. My training includes 192 hours of training sponsored by the United States Secret Service on digital evidence and computer forensics examinations. I have over 300 hours of training recognized and certified by the Illinois Training and Standards Board and have been trained in the investigation of computer use in the exploitation of children as well as other digital investigations and evidence gathering. I am a member of the Illinois Attorney General's Internet Crimes Against Children Task Force. I have assisted Federal, State, and local agencies in digital investigations. I have, on several occasions, been involved with investigations involving internet/computer crimes and have been involved in the execution of numerous search warrants.

2. I make this affidavit in support of a warrant to search an LG Model US670 cellular telephone (S/N: 103KPRW0111358) with the markings "Made in Korea", which was seized on 05/10/13 during an authorized undercover operation at 300 N. Jefferson St. Apartment #3, Jerseyville, Illinois 62052, which is located in the Southern District of Illinois.

3. This affidavit seeks to search for contraband, evidence or instrumentalities of violations of Title 18 U.S.C. § 2422(b), specifically evidence related to the enticement of a minor.

4. The statements contained in this affidavit are based upon my training and experience as a Special Federal Officer of the United States Secret Service, information provided to me by other law enforcement officers and investigators, and upon my consultation with personnel trained in the investigation, seizure, and analysis of computers, electronic data, and electronic media. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are

necessary to establish probable cause to believe that evidence of a violation of Title 18 U.S.C. § 2422(b) on the LG Model US670 cellular telephone (S/N: 103KPRW0111358).

Cellular Phone/Computer Searches Generally

5. It is my belief that any number of the items sought in this affidavit for search warrant, may be found which were stored electronically. Based upon my knowledge, training, and experience, I know that data in digital form can be stored on a variety of systems and storage devices, including cellular phones, hard disk drives, floppy disks, compact disks, magnetic tapes, flash drives, and memory chips. Some of these devices can be smaller than a thumbnail and can take several forms, including thumb drives, secure digital media used in phones and cameras, personal music devices, and similar items. I know that electronic files can be easily moved from one computer or electronic storage medium to another. Therefore, electronic files downloaded to or created on one computer can be copied on or transferred to any other computer or storage medium at the same location. In addition, I know that searching computerized information for evidence of crimes often requires Special Agents to seize most or all of a computer system's central processing unit ("CPU") and/or laptop computer, input/output peripheral devices, related software, documentation, storage media, and data security devices, including passwords, so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. This is true because of the following:

- a. Volume of evidence: Electronic media and storage devices such as cellular phone, hard disks, CD-ROMs, DVDs, diskettes, and tapes can store the equivalent of thousands of pages of information. Additionally, a suspect may try to conceal criminal evidence by storing it in random order with deceptive file names. This may require searching authorities to examine all of the stored data to determine which particular files is evidence or instrumentalities of crime. This sorting process can take weeks to months, depending on the volume of data stored. It would also be impractical to attempt this type

of data search on site.

b. Technical requirements: Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment.

The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert and examiner is qualified to analyze the system and its data. In any event, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password protected, or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional modification or destruction (either from external sources or from destructive code embedded in the system such as a “booby trap”), a controlled environment is essential to its complete and accurate analysis.

c. The analysis of electronically stored data, whether performed on-site or in a laboratory or other controlled environment, may entail any or all of several different techniques. Such techniques may include, but shall not be limited to, surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for the pertinent files, in order to locate the evidence and instrumentalities authorized for seizure by the warrant); “opening” or reading the first few “pages” of such files in order to determine their precise contents; “scanning” storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; or performing electronic “keyword” searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.

d. Latent data: Searching digital devices can require the use of precise, scientific procedures designed to maintain the integrity of the evidence and to recover latent data. The recovery of such data may require the use of special software and procedures. Data

that represents electronic files or remnants of such files can be recovered months or even years after it has been downloaded onto a hard drive, deleted, or viewed via the Internet. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in space on the hard drive or other storage media that is not allocated to an active file. In addition, a computer's operating system may also keep a record of deleted data in a swap or recovery file or in a program specifically designed to restore the computer's settings in the event of a system failure.

e. Contextual data: In some instances, the device "writes" to storage media without the specific knowledge or permission of the user. Generally, data or files that have been received via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to such data or files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve artifacts of electronic activity from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer usage. Logs of access to websites, file management/transfer programs, firewall permissions, and other data assist the examiner and investigators in creating a "picture" of what the computer was doing and how it was being used during the relevant time in question. Given the interrelationships of the data to various parts of the computer's operation, this information cannot be easily segregated.

6. Digital data on the hard drive that is not currently associated with any file, may reveal evidence of a file that was once on the hard drive but has since been deleted or edited, or it could reveal a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, email programs, and chat programs store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations.

7. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be learned from the absence of particular data on a digital device. Specifically, the lack of computer security software, virus protection, malicious software, evidence of remote control by another computer system, or other programs or software may assist in identifying the user indirectly and may provide evidence excluding other causes for the presence or absence of items sought by this application. Additionally, since computer drives may store artifacts from the installation of software that are no longer active, evidence of the historical presence of the kind of software and data described may have special significance in establishing timelines of usage, confirming the identification of certain users, establishing a point of reference for usage, and, in some cases, assisting in the identification of certain users. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Evidence of the absence of particular data on the drive is not generally capable of being segregated from the rest of the data on the drive.

Background of Investigation

8. On May 7, 2013, I, Special Agent David Wargo of the Illinois State Police, assigned to the USSS Southern Illinois Cyber-crime Unit, received a report that a subject was

attempting to solicit a minor child for the purpose of having sex with the minor child. The individual who initially contacted us will be referred to herein as CW-1.

9. A subject, whom CW-1 knows as DAVE DRISKILL was sending text messages to CW-1 via cellular phone from a cellular phone number of 618-556-8444. CW-1 resides at 23509 Appletree Lane, Elsah, Illinois, within the Southern District of Illinois.

10. On May 7, 2013, I, along with Special Agent Patrick McGuire of the Illinois State Police met with CW-1 at the Jerseyville Police Department for an audio/video recorded statement.

11. During the video recorded interview, CW-1 stated that she was contacted via text message on 05/01/2013 by a subject she knows as DAVE DRISKILL. The message asked CW-1 if she wanted to do business and make some money, and offered three thousand for a “seven to eleven”, CW-1 did not reply. CW-1 stated she believed DRISKILL was requesting her to provide a 7 to 11 year old child he could have sex with. On 05/02/2013 DRISKILL sent another message stating “four thousand”, CW-1 did not reply and contacted the Jersey County Sheriff’s Department. CW-1 stated she believed DRISKILL had contacted her for this request because in July of 2012 DRISKILL had a similar request of CW-1 to find an 18 year old female that DRISKILL could go out with for a night. CW-1 stated she located a female who she believed was 19 or 20 years old at the time, who agreed to go out with DRISKILL.

12. CW-1 stated she has known DRISKILL for approximately six years. CW-1 stated DRISKILL is a friend of her ex-boyfriend’s father. CW-1 stated that approximately 3 years earlier, DRISKILL had lived with her, her children and her boyfriend for approximately three months.

13. During the recorded interview, I asked CW-1 to send a text message from her Apple i-Phone to DRISKILL'S cellular phone (618-556-8444). The message stated CW-1 knows a guy who may be able to help him out and provided a contact number where he could be reached. I utilized a covert name, "KEVIN," and number for the purposes of the investigation.

14. DRISKILL insisted on only dealing through CW-1. Several text messages were sent back and forth between DRISKILL and CW-1 between May 7, 2013 and May 10, 2013. Through the course of these text messages, CW-1 told DRISKILL that "Kevin" had a 7 year old girl he would make available. DRISKILL sent a text message saying he wanted to touch, lick and rub against "KEVIN'S" girl. DRISKILL offered \$1,500 for "KEVIN'S" girl. DRISKILL repeatedly asked for pictures of KEVIN'S girl in various states of dress, specifically requesting a picture of her in bra and panties and one without panties. DRISKILL also repeatedly asked for a picture of CW-1's nine year old daughter. Specifically, DRISKILL asked for a picture of her exposed genitalia and offered \$500 for the picture. Eventually, DRISKILL requested that "KEVIN" call him.

15. On May 7, 2013 at approximately 10:56 p.m., acting as "KEVIN," I contacted DRISKILL, stating I was "KEVIN" and asked for "DAVE." The subject on the phone stated he was "DAVE" and asked the name of my daughter, to which I replied "CHRISTINE." I asked DAVE how much he was willing to pay and he stated fifteen hundred. I then asked if he was going to wear a condom and he stated he would. During the conversation, DAVE asked on more than one occasion if CHRISTINE was going to be upset. After the second time, I replied "she's not going to cry if that's what you mean". The phone conversation ended with DAVE stating he would contact CW-1 in the morning.

16. No text conversation occurred on May 8, 2013.

17. On May 9, 2013, DRISKILL contacted CW-1 via text message, stating the fifteen hundred offer was still on the table. CW-1 contacted me via telephone. Myself, CW-1 and S/A McGuire engaged DRISKILL in a text conversation which focused on "KEVIN" having a seven year old daughter available for sex. On May 10, 2013, through text messages, a meeting place was agreed upon and a time for the meeting was set for 3:30 p.m.

18. The meeting place was arranged for 300 North Jefferson Apartment 3 in Jerseyville, Illinois, which is in the Southern District of Illinois.

19. A records check indicated that the phone number 618-556-8444 was issued to U.S. Cellular.

20. On May 10, 2013 a subpoena was issued by the Jersey County State's Attorney's Office to U.S. Cellular for subscriber records for telephone number 618-556-8444. I contacted U.S. Cellular, via telephone, after they received the subpoena and was advised the U.S. Cellular subscriber issued number 618-556-8444 was DAVID DRISKILL.

21. On May 10, 2013 at approximately 2:29 p.m. DRISKILL sent a text message to CW-1 stating he was getting lubricant.

22. At approximately 3:20 p.m., CW-1 and I were seated in separate chairs in a chair in front of apartment 3 at 300 North Jefferson Street in Jerseyville, Illinois. I observed an older male subject who appeared to be, based on the driver's license picture I had seen, DAVID DRISKILL, approach the front door of apartment 3. I introduced myself as "KEVIN". I asked the male subject if he was "DAVE" and he replied "yes" (subject was later identified by Illinois Driver's License as DAVID G. DRISKILL). I asked if he brought the money and he replied "is she inside." I stated she was, and again asked for the money. DRISKILL handed me \$1,500

cash. I sat back down in the chair and told DRISKILL she was inside. DRISKILL then opened the door to apartment 3 and stepped inside the apartment.

23. DRISKILL was met inside the apartment by United States Secret Service Agents DEREK DAVIS and CHRISTOPHER WILLIAMS and MAJOR ROGER KIRBY of the Jerseyville Police Department. DRISKILL was taken into custody without incident.

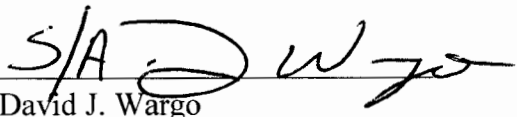
24. Upon his arrest an LG Model US670 cellular telephone (S/N: 103KPRW0111358) with the markings "Made in Korea," a condom and an unopened box containing KY lubricant was seized from his person and taken into evidence. DRISKILL gave verbal consent to search the vehicle he had driven to the location.

25. DRISKILL was interviewed at the Jersey County Sheriff's Department by me and S/A McGuire. Shortly into the interview, DRISKILL requested an attorney and all questioning ceased. As I was walking out of the interview room, DRISKILL spontaneously stated "I've never done anything like this before in my life".

Conclusion

26. Based on the foregoing information, I have probable cause to believe that evidence of violations of 18 U.S.C. § 2422(b), as set forth herein and in Attachment A, are currently on the property of one LG Model US670 cellular telephone (S/N: 103KPRW0111358). I therefore respectfully request that a search warrant be issued authorizing the search for and seizure of the items set forth in Attachment A.

FURTHER AFFIANT SAYETH NAUGHT.



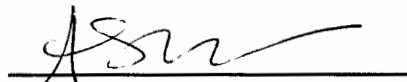
David J. Wargo

Special Federal Officer

USSS Southern Illinois Cyber-crime Unit

STEPHEN R. WIGGINTON

United States Attorney



ALI SUMMERS

Assistant United States Attorney

State of Illinois)
) SS.
County of Jersey)

Sworn to before me and subscribed in my presence on this 17th day of MAY, 2013, at East St. Louis, Illinois.



CLIFFORD J. PROUD

United States Magistrate Judge

ATTACHMENT A

- (a) Any and all text messages, photos videos, call logs and other data pertaining to the operation of phone.
- (b) Any and all documents, records, e-mails, and internet history (in documentary or electronic form) pertaining to enticement of a child or visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256, or pertaining to an interest in the enticement of a minor.
- (c) Electronic chat room and mail messages, notes, listings, and records relating to other individuals or entities involved in enticement of a minor, or receipt of materials that depict or promote the sexual exploitation of children.
- (d) Visual depictions in whatever form created, stored, or printed which depict children under the age of 18 years engaged in sexually explicit conduct.